DEPARTMENT OF THE NAVY
COMMANDER MOBILE MINE ASSEMBLY GROUP
2536 FOURTH STREET
N. CHARLESTON, S.C. 29406-6171

IN REPLY REFER TO:
COMOMAG/MOMAGINST 5230.1C CH-
Code N01F
21 MAR 95

COMOMAG/MOMAG INSTRUCTION 5230.1C CHANGE TRANSMITTAL TWO

Subj: UTILIZATION OF AUTOMATED INFORMATION SYSTEMS (AIS)

Encl: (1) Revised pages 6 and 7 of basic instruction
(2) Revised enclosure (5) to basic instruction

1. Purpose. To promulgate Change Two, to the basic instruction.

2. Action

a. Remove pages 6 and 7 and enclosure (5) from the basic instruction and replace with enclosures (1) and (2).

b. Pen and ink change "Encl: (5)" on cover page to read "Sample Accreditation Letter with AIS Accreditation Checklist," vice "Sample Accreditation Letter."

D. J. POWERS

Distribution:
COMOMAG/MOMAGINST 5216.1N
List II, Case A
COMINEWARCOM (N6)

(5) Reporting all breaches of terminal security to the host activity and the ADPSO.

7. Security. References (a) through (d) specify the policies, procedures and responsibilities for establishing and maintaining AIS security programs within the Navy and will be adhered to by COMOMAG and its subordinate commands.

a. Training. All personnel who utilize AIS equipment will receive an AIS security brief from the ADPSO within 30 days of reporting to a MOMAG activity. In addition, all users will receive annual AIS security training.

b. Accreditation. Accreditation is a formal authorization statement by a Designated Approval Authority (DAA) to operate an AIS or computer network in an environment which provides processing security commensurate with a set of security requirements derived from an approved risk management process. Each computer system and computer network installed at a MOMAG facility will be assigned a system ID which includes the department abbreviation plus a sequential number (i.e., OPS-01). Each system will be accredited in accordance with procedures outlined in reference (b). Systems which have identical configurations and processing requirements may be grouped for accreditation. The AIS accreditation checklist outlined in enclosure (5) shall be used as a guide for the accreditation process. A copy of the accreditation letter shall be forwarded to COMOMAG and shall conform to the format outlined in enclosure (5). All AIS and computer networks which process sensitive unclassified or classified data must meet C2 trust level requirements to be accredited. All accreditations will be reviewed once every three years or whenever significant changes occur in system functionally, architecture or processing environment. At a minimum, the following risk management process will be completed before accreditation is granted:

(1) Security Survey. The Security Survey contained in chapter (5) of enclosure (2) to reference (b) will be completed for each AIS and computer network. An automated version of this form may be utilized where available.

(2) Activity AIS Security Plan. An Activity AIS Security Plan (AAISSP) will be developed for the activity in accordance with chapter (7) of enclosure (2) to reference (b). Once the Security Survey and AAISSP are completed, the DAA will be requested to issue an Interim Authority To Operate (IATO) for those systems whose risk levels are considered acceptable. Such authority shall not exceed one year.

(3) TEMPEST. Reference (f) excludes all MOMAG activities from TEMPEST review requirements. However, COMOMAG and the MOMAG sites will observe proper TEMPEST profiles in accordance with paragraph 7c of this instruction.

(4) Contingency Plan. COMOMAG and the MOMAG sites will develop a command AIS Contingency Plan which defines emergency backup processing and recovery procedures for each AIS or computer network on which mission critical applications are processed. Mission critical applications are applications which could unduly hinder or prevent an activity from meeting its mission objectives if they were not available

and include such routines as MTF Editor, MDU, MDS, GATEGUARD, SCAAIR, DAMES and similar systems. Systems on which no mission critical applications are performed shall be identified in the plan as having no contingency requirement. Each Contingency Plan will follow the sample outlined in enclosure (6) and will:

(a) Identify those persons responsible for carrying out each action.

(b) Identify the systems and equipment involved.

(c) Identify the software, supplies and documentation required.

(d) Identify an off-site backup processing and storage facility where backup processing support can be obtained and copies of all required software, supplies and documentation can be stored. COs/OICs will negotiate off-site support agreements with other activities in their locality.

(e) Outline preparations required prior to a disruption of services.

(f) Specify the emergency backup and recovery procedures to be followed in the event of temporary disruptions, partial loss of assets and/or facility and total loss of assets and/or facility.

(5) Security Test and Evaluation. An abbreviated Security Test and Evaluation (ST&E) as defined in Chapter 10 of enclosure (2) to reference (b) will be completed and submitted as part of the accreditation request to the DAA. The Security Test and Evaluation checklist outlined in reference (b) shall be used to conduct the ST&E.

(6) Accreditation Report. An accreditation report will be drafted and stored with other support documentation.

(7) Accreditation Support Package. An accreditation support package containing copies of all documentation generated in the risk management process will be assembled and retained by the ADPSO.

c. TEMPEST Requirements. Reference (h) exempts COMOMAG and the MOMAG sites from TEMPEST review requirements. However, all MOMAG activities will continue to observe proper TEMPEST profiles for those AISs on which classified data is processed. To ensure the most suitable TEMPEST environment is maintained, each CO/OIC will utilize the following guidelines for selecting and placing AIS equipment on-site:

(1) Systems with removable hard drives will be utilized for classified processing unless specifically authorized by COMOMAG. The security and disposal measures outlined in paragraph 7(o) of this instruction will be implemented for all hard drives, removable or fixed, which contain classified data.

(2) Locate the system in an area in which a 16 to 20 meter distance from the system could reasonably be considered controlled (i.e., under constant surveillance).

SAMPLE ACCREDITATION LETTER

From: Commanding Officer/Officer in Charge, Mobile Mine Assembly Group Unit/Detachment _____
To: ADP Security Officer

Subj: LETTER OF ACCREDITATION

Encl: (1) AIS ACCREDITATION CHECKLIST

Ref: (a) OPNAVINST 5239.1A
(b) OMOMAGINST 5230.1C
(c) COMMAND SECURITY INSTRUCTION

1. In accordance with references (a) through (c), the following ADP systems within this command have a completed risk assessment, Security Test and Evaluation (ST&E) and contingency plan and are fully accredited to operate in the security mode and classification level specified for a period not to exceed (expiration date).

SYSTEM ID	CLASSIFICATION LEVEL	MODE OF OPERATION

CO/OIC Signature

AIS ACCREDITATION CHECKLIST

_ Define duties and responsibilities of the ADPSO.
_ Define duties and responsibilities of the ADPSSOs.
_ Define duties and responsibilities of the TASOs.
_ Appoint an ADPSO to serve as focal point for all activity AIS security matters.
_ Define class and type of information processed on AISs.
_ Appoint Tempest Control Officer for Classified Information Processing Systems (as required)..
_ Prepare and submit security plan for AISs preparing sensitive unclassified information.
_ Define budgetary requirements for implementation and maintenance of the program.
_ Train APD Security Staff for their roles.
_ Develop and implement an AIS Security Training and Awareness Program for all activity personnel.
_ Develop Standard Operating procedures for each AIS.
_ Implement the Risk Management Program by completing accreditation action items.
_ Conduct AIS Security Survey(s)..
_ Develop Activity AIS Security..
_ Issue Interim Authority to Operate (IATO).
_ Implement minimum program requirements.
_ Conduct Risk Analysis.
_ Develop Security Test and Evaluation Plan and execute tests.
_ Develop and test Contingency Plan.
_ Compile accreditation report.
_ Issue accreditation statement.

Enclosure (1)